

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-332742

(43)Date of publication of application : 30.11.2000

(51)Int.Cl.

H04L 9/08

G06F 12/14

G09C 1/00

G11B 20/10

H04L 9/32

(21)Application number : 11-136695

(71)Applicant : **SONY CORP**

(22) Date of filing : 18.05.1999

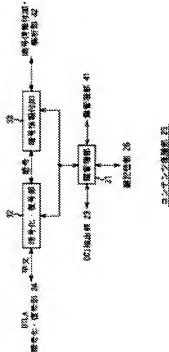
(72)Inventor : HAMADA ICHIRO
FUJII ASAKO

(54) INFORMATION PROCESSING UNIT, METHOD THEREFOR AND SERVING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To deter unauthorized use of contents.

SOLUTION: A key management section 31 discriminates whether an authentication key of an application is regular and controls a contents protection section 25 to execute transmission/reception of the contents of the application, only when the key management section 31 decides that the contents are regular. An encrypting/decoding section 32 enciphers the decoded contents by using an cryptographic key entered from the key management section 31 and provides an output of the result to a cipher information adding section 33. The cipher information adding section 33 adds cipher information to the ciphered contents from the ciphering and deciphering section 32 to provide an output of the result to the application.



[Detailed Description of the Invention]

[0001] [Field of the Invention]About information processing equipment, a method, and a distribution medium, especially this invention is used, when deterring the illegal use of contents, and it relates to suitable information processing equipment, a method, and a distribution medium.

[0002] [Description of the Prior Art]the contents (for example, the audio information currently recorded on CD (Compact Disc).) from which copyright is protected conventionally In order to deter that the AV information etc. which are recorded on DVD (Digital Versatile Disc) are reproduced unjustly, To the equipment which can record contents (for example, MD (Mini Disc) recorder, a CD-R recorder, DV (Digital Video) recorder, etc.). SCMS (Serial Copy Management System) or CGMS (Copy Generation Management System) is adopted. In SCMS or CGMS, predetermined information was added to contents and the number of times which can be copied is restricted based on the information.

[0003]It became possible to communicate contents via an IEEE1394 bus these days between the AV device and personal computer which reproduce or record contents. In the personal computer, the contents mentioned above were played and recorded with improvement in the speed of CPU (Central Processing Unit), or large-scale-izing of a hard disk, and it became possible to edit further.

[0004] [Problem to be solved by the invention]Therefore, when an inaccurate application program which alters intentionally the information added to the contents mentioned above was installed in the personal computer, the problem which cannot deter that contents will be copied illegally occurred.

[0005]In [this invention is made in view of such a situation, and] a personal computer, It enables it to deter the illegal use of the contents using an inaccurate application program by enciphering contents just before an application program is supplied.

[0006] [Means for solving problem]written this invention is characterized by it having been alike and comprising the following at Claim 1.

The encryption key creating means which generates an encryption key using the source key corresponding to the copyright information added to the contents inputted.

The encoding means which enciphers contents using an encryption key.

The judging means which judges the justification of an application program using the authentication key inputted from an application program.

The secret key generating means which generates a secret key using the authentication key inputted from an application program, The feeding means which supplies the encryption key enciphered using the secret key which the secret key generating means generated, and the contents enciphered by the encoding means to an application program corresponding to the decided result of a judging means.

[0007][0007]. ***** is characterized by it having been alike and comprising the following.

The encryption key with which a disposal method generates an encryption key using the source key corresponding to the copyright information added to the contents inputted.

Dark which enciphers contents as a step using an encryption key.

The justification of an application program is judged using the authentication key inputted as a step from an application program.

A step and the secret key generation step which generates a secret key using the authentication key inputted from an application program, The encryption key enciphered using the secret key generated by the secret key generation step and the contents enciphered at the encryption step are supplied to an application program corresponding to the decided result of a determination step.

[0008]The encryption key generation step which generates an encryption key using the source key corresponding to the copyright information added to the contents into which the distribution medium according to claim 4 is inputted, The encryption step which enciphers contents using an encryption key, and the determination step which judges the justification of an application program using the authentication key inputted from an application program, The secret key generation step which generates a secret key using the authentication key inputted from an application program, The encryption key enciphered using the secret key generated by the secret key generation step and the contents enciphered at the encryption step are corresponded to the decided result of a determination step, The program which the computer which makes information processing equipment perform processing containing the supply step supplied to an application program can read is provided.

[0009]In the information processing equipment according to claim 1, the information processing method according to claim 3, and the distribution medium according to claim 4, an encryption key is generated using the source key corresponding to the copyright information added to the contents inputted, and contents are enciphered using an encryption key. A secret key is generated using the authentication key inputted from an application program, the justification of an application program is judged, and it corresponds to the decided result, The encryption key enciphered using the secret key and the contents enciphered are supplied to an application program.

[0010] [Mode for carrying out the invention]The example of composition of the personal computer which applied this invention is explained with reference to drawing 1. This personal computer (PC) 1 is connected with the apparatus (for example, the DV recorder (DVR) 3 as shown in drawing 1, the set top box (STB) 4, and hard disk (HDD) 5 grade) which can treat contents via IEEE1394 bus 2. The contents which communicate via IEEE1394 bus 2, CPTWG (CopyProtection.) The system to which the license management company DTLA (Digital Transmission Licensing Administrator) recommended by TechnicalWorking Group licenses (hereafter) It is based on describing it as a DTLA system, and is enciphered.

[0011]The personal computer 1 comprises the IEEE1394 interface 11 connected via the bus 16, CPU12, RAM13, ROM14, and the hard disk 15. The IEEE1394 interface 11 via IEEE1394 bus 2, . Start the contents inputted from other apparatus (DVR3 grade) with the personal computer 1. The application program (the application program in which reproduction, record, edit, etc. are possible is only hereafter described to be application to the contents started) in which reproduction, record, edit, etc. are possible is supplied to contents. The IEEE1394 interface 11 outputs the contents which application processed to other apparatus via IEEE1394 bus 2.

[0012]The application program is memorized by the hard disk 15, by the control of CPU12 based on BIOS memorized by ROM14, is transmitted to RAM13 and started. Although the peculiar authentication key Kn is given from the administrator of a ciphering system like DTLA to this application program, In order to obtain this authentication key Kn, in the work origin of an application program, a user needs to vow in a contract etc. not using unjustly the contents from which copyright is protected. The

term of a system as used herein means the overall equipment constituted by two or more equipment, a means, etc.

[0013]Here, the binary used as ID and the pair of Signature is contained in the authentication key Kn, and the result of having applied the predetermined computing equation to one side serves as another side. It can check that it is a right pair by applying a predetermined computing equation to both sides. Only the lock management department 31 (drawing 3) knows this predetermined computing equation, namely, can judge the justification of the authentication key Kn. Since it is dramatically difficult to ask for a predetermined computing equation by the inverse operation using ID and Signature, it is impossible to forge the authentication key Kn as a matter of fact.

[0014]Drawing 2 shows the detailed example of composition of the IEEE1394 interface 11. The control section 21 controls each part of the IEEE1394 interface 11. The input output section 22 receives the contents enciphered by the DTLA system inputted from IEEE1394 bus 2, and outputs them to the CCI (Copy Control Information) primary detecting element 23. Although the CCI primary detecting element 23 supplies the contents inputted from the input output section 22 to DTLA encryption and the decoding part 24, in that case, it detects CCI (2 bits) currently recorded on the header of contents, and supplies the control section 21, DTLA encryption and a decoding part 24, and the contents protecting part 25.

[0015]CCI is information which shows control of the copy permitted to the contents to which self is added, and there are four kinds of State, 00, 10, 01, and 11. When CCI is 00 (Copy free), it means that the copy of the number of times of unrestricted is permitted to corresponding contents. When the State of CCI is 10 (One Generator Copy Possible), it means that the copy is permitted only once to corresponding contents. When the State of CCI is 01 (No More Copy), the State of CCI is what reproduced the contents which are 10 (the 2nd generation), and corresponding contents mean that the copy is not permitted to this. When the State of CCI is 11 (Never copy), it means that the copy is not permitted to corresponding contents.

[0016]DTLA encryption and the decoding part 24 decode the contents enciphered by the DTLA system inputted from the CCI primary detecting element 23, and outputs them to the contents protecting part 25. A DTLA system uses DTLA encryption and the

decoding part 24, it enciphers, and outputs the contents inputted from the contents protecting part 25 to the input output section 22. The encryption and decoding in DTLA encryption and the decoding part 24 are performed after the mutual recognition work defined by the DTLA system between DTLA encryption and the decoding part 24, and the equipment (DVR3 grade) that outputted contents is completed.

[0017]The contents protecting part 25 enciphers the contents inputted from DTLA encryption and the decoding part 24, and supplies them to application. The contents protecting part 25 decodes the contents which are inputted from application and which are enciphered, and supplies them to DTLA encryption and the decoding part 24. The key storage part 26 has memorized two or more source keys Ks used for the encryption processing in the contents protecting part 25 for every State of CCI.

[0018]Drawing 3 shows the detailed example of composition of the contents protecting part 25. Only when it judges with the lock management department 31 judging whether the authentication key Kn inputted from the lock management department 41 (drawing 4) of application is regular, and its authentication key Kn being regular, each part of the contents protecting part 25 is controlled to perform transfer of contents with application.

[0019]Namely, the lock management department 31 applies a predetermined computing equation to ID contained in the authentication key Kn from application, When it judged whether it would be equal to Signature to which the result corresponds and judges with the result of an operation being equal to Signature (the authentication key Kn is regular), By applying a predetermined computing equation to ID and Signature, When it judges whether it is a right pair and judges with it being a right pair, the source key Ks corresponding to the State of CCI inputted from the CCI primary detecting element 23 is read, the encryption key Kc is generated using the source key Ks and a random number, and encryption and the decoding part 32 are supplied. The encryption key Kc is updated by predetermined every cycle (for example, for 30 seconds thru/or for 120 seconds). Whenever the lock management department 31 updates the encryption key Kc, it outputs the State of CCI to the coding information adjunct 33. The lock management department 31 generates the secret key Ka based on the information for secret key Ka calculation, including the authentication key etc. which are inputted from the lock management department 41 of application, enciphers using the secret key Ka

and outputs the encryption key Kc to the lock management department 41.

[0020]Encryption and the decoding part 32 encipher using the encryption key Kc from the lock management department 31, and outputs the contents decoded from DTLA encryption and the decoding part 24 to the coding information adjunct 33. Encryption and the decoding part 32 decode the contents enciphered from the coding information adjunct 33, and outputs them to DTLA encryption and the decoding part 24.

[0021]The coding information adjunct 33 adds the coding information of even changed to them whenever the State (2 bits) of CCI and the encryption key Kc are updated by the contents enciphered from encryption and the decoding part 32, or odd (1 bit), It outputs to the coding information analyzing parts 42 (drawing 4) of application. The coding information adjunct 33 outputs the contents enciphered from the coding information analyzing parts 42 to encryption and the decoding part 32.

[0022]Drawing 4 shows the functional block diagram of the application in which reproduction, record, edit, etc. are possible to contents. The lock management department 41 outputs the memorized authentication key Kn to the lock management department 31 of the contents protecting part 25 with the information for secret key Ka calculation, before it has memorized the authentication key Kn given to the application program and application starts transfer of contents. The lock management department 41 corresponds to the information which shows whether the information (even or odd) which shows renewal of the encryption key Kc which is inputted from the coding information analyzing parts 42, and which is contained in coding information was changed, The encryption key Kc enciphered with the secret key Ka from the lock management department 31 is decoded, and it outputs to encryption and the decoding part 43.

[0023]The coding information analyzing parts 42 output the contents which are inputted from the coding information adjunct 33 and which are enciphered with the encryption key Kc to encryption and the decoding part 43, and output the coding information added to the lock management department 41. The coding information analyzing parts 42 output the contents enciphered from encryption and the decoding part 43 to the coding information adjunct 33.

[0024]Encryption and the decoding part 43 decode the contents enciphered with the

encryption key Kc inputted from the coding information analyzing parts 42 using the encryption key Kc from the lock management department 41, and outputs them to the contents treating part 44. Encryption and the decoding part 43 encipher the contents inputted from the contents treating part 44, and outputs them to the coding information analyzing parts 42.

[0025]The contents treating part 44 performs processings (reproduction, record, or edit) corresponding to a user's operation to the inputted contents. Since CCI contained in the coding information which the coding information analyzing parts 42 analyzed is supplied to the contents treating part 44, in the contents treating part 44, processings (copy exceeding restricted frequency, etc.) which are contrary to CCI are not performed.

[0026]If the IEEE1394 interface 11 is realized by one LSI (Large Scale Integrated circuit), it will become possible to deter a malfeasance which reads the contents decoded from the middle of the circuit.

[0027]Next, the processing which inputs contents into application is explained with reference to the flow chart of drawing 5. The contents as which this input process is enciphered by the IEEE1394 interface 11 by the DTLA system are inputted, The CCI is detected in the CCI primary detecting element 23, and is inputted into the lock management department 31 of the contents protecting part 25, and after the contents enciphered by the DTLA system are decoded by DTLA encryption and the decoding part 24 and are inputted into encryption and the decoding part 32 of the contents protecting part 25, it performs.

[0028]In Step S1, the lock management department 41 of application outputs the demand of a contents input, the memorized authentication key Kn, and the information for secret key Ka calculation, and the lock management department 31 of the contents protecting part 25 receives them.

[0029]In Step S2, when it judges whether the authentication key Kn from the lock management department 41 is regular and judges with the authentication key Kn being regular, he follows the lock management department 31 to Step S3.

[0030]In Step S3, the lock management department 31 reads the source key Ks corresponding to the State of CCI from the key storage part 26, generates the encryption key Kc using the source key Ks and a random number, and outputs it to

encryption and the decoding part 32. The lock management department 31 resets to 0 the timer which measures the timing which updates the encryption key Kc.

[0031]In step S4, the lock management department 31 generates the secret key Ka using the information for secret key Ka calculation, further, enciphers the encryption key Kc using the secret key Ka, and outputs it to the lock management department 41 of application. The lock management department 41 decodes the encryption key Kc.

[0032]In Step S5, encryption and the decoding part 32 encipher using the encryption key Kc from the lock management department 31, and outputs the contents decoded from DTLA encryption and the decoding part 24 to the coding information adjunct 33.

[0033]In Step S6, the coding information adjunct 33, The coding information which comprises the information (in now the encryption key Kc is even since it is not updated) which shows the State of CCI and renewal of the encryption key Kc is generated, and it adds to the contents enciphered from encryption and the decoding part 32, and outputs to the coding information analyzing parts 42 of application. The coding information analyzing parts 42 judge whether the information which shows the renewal of the encryption key Kc included in coding information is changed, and output a decided result to the lock management department 41. The lock management department 41 supplies the present encryption key Kc to encryption and the decoding part 43 based on this decided result. Encryption and the decoding part 43 decode contents using the encryption key Kc, and outputs them to the contents treating part 44.

[0034]In Step S7, when it judges whether all the contents were outputted to application from the contents protecting part 25 and judges with outputting no contents, he follows the lock management department 31 to Step S8. In Step S8, by referring to a self timer, the lock management department 31 detects time when the present encryption key Kc is used, and judges whether the time went through predetermined time (for 30 seconds thru/or for 120 seconds). When judged with time when the present encryption key Kc is used not having gone through predetermined time, it returns to Step S5 and processing after it is repeated.

[0035]Then, in Step S8, when it judges that a hour of use of the present encryption key Kc went through predetermined time, it progresses to step S9. In step S9, the lock management department 31 generates the encryption key Kc using the source key Ks

and a random number generated again (updating), and outputs it to encryption and the decoding part 32. The lock management department 31 resets a self timer to 0.

[0036]Then, it returns to step S4, and subsequent processings are repeated until it is judged with having outputted all the contents at Step S7. However, since the encryption key Kc is updated by step S9, information which shows renewal of the encryption key Kc included in coding information added at Step S6 is changed from even to odd. Corresponding to information which shows renewal of this encryption key Kc, the encryption key Kc supplied to encryption and the decoding part 32 from the lock management department 41 is also updated.

[0037]In Step S2, when judged with the authentication key Kn not being regular, it progresses to Step S10. In Step S10, the lock management department 31 reports that it cannot be attested to the lock management department 41 of application.

[0038]Next, the processing which outputs the contents processed with application to IEEE1394 bus 2 is explained with reference to the flow chart of drawing 6. This output process is performed after the contents edited in the contents treating part 44 of application are inputted into encryption and the decoding part 43.

[0039]In Step S21, the lock management department 41 of application outputs the State of CCI set up to the demand of a contents output, the memorized authentication key Kn, the information for secret key Ka calculation, and the contents to output to the lock management department 31 of the contents protecting part 25.

[0040]In Step S22, when it judges whether the authentication key Kn from the lock management department 41 is regular and judges with the authentication key Kn being regular, he follows the lock management department 31 to Step S23.

[0041]In Step S23, the lock management department 31 reads the source key Ks corresponding to the State of CCI inputted from the lock management department 41 from the key storage part 26, generates the encryption key Kc using the source key Ks and a random number, and supplies it to encryption and the decoding part 32. In Step S24, the lock management department 31 generates the secret key Ka using the information for secret key Ka calculation from the lock management department 41, enciphers further the encryption key Kc generated at Step S22 using the secret key Ka, and outputs it to the lock management department 41 of application. The lock

management department 41 decodes the encryption key Kc, and outputs it to encryption and the decoding part 43.

[0042]In Step S25, encryption and the decoding part 43 of application encipher the contents inputted from the contents treating part 44 using the encryption key Kc from the lock management department 41, and outputs them to encryption and the decoding part 32 via the coding information analyzing parts 42 and the coding information adjunct 33.

[0043]In Step S26, encryption and the decoding part 32 decode the contents enciphered from application (encryption and decoding part 43) using the encryption key Kc inputted from the lock management department 31 at Step S23, and outputs them to DTLA encryption and the decoding part 24.

[0044]In Step S27, DTLA encryption and the decoding part 24 encipher by a DTLA system, and outputs the contents which were inputted from encryption and the decoding part 32 of the contents protecting part 25 and which are decoded to the input output section 22.

[0045]In Step S28, the input output section 22 outputs the contents enciphered by the DTLA system from DTLA encryption and the decoding part 24 to IEEE1394 bus 2.

[0046]In Step S22, when judged with the authentication key Kn not being regular, it progresses to Step S29. In Step S29, the lock management department 31 reports that it cannot be attested to the lock management department 41 of application.

[0047]It may be made to change the encryption key Kc periodically like the input process mentioned above also in this output process.

[0048]as mentioned above, according to this embodiment, boil the contents protecting part 25 of the IEEE1394 interface 11 only to application with the regular authentication key Kn to deliver and receive contents -- now, *****. However, the application which can perform the illegal copy of contents, etc. acquires the regular authentication key Kn by a certain method, and it is also considered that contents will be used unjustly. In then, the lock management department 31 of the contents protecting part 25 which judges the justification of the authentication key Kn in this invention. Make the RIBOKESHON list in which the authentication key Kn used unjustly is registered memorize, and in the case of authenticating processing the lock management

department 31, In addition to the judgment of the compatibility of ID contained in the authentication key Kn, and Signature, it is made to perform collation with a RIBOKESHON list, It is made as [judge / with the authentication key Kn registered into the RIBOKESHON list being regular even if ID and Signature serve as a pair].

[0049]About this RIBOKESHON list, how to distribute that newest thing to the lock management department 31 via the network of the Internet or IEEE1394 bus 2 grade can be considered. As a utilizing method of this RIBOKESHON list, how to register the authentication key Kn separately, and the methods (for example, the predetermined bit by the side of MSB (Most Significant Bit) of ID of the authentication key Kn is specified) of registering two or more authentication keys Kn collectively can be considered. It becomes possible to make it judge that all the applications which the specific software maker (software maker where the violation to the agreement vowed when acquiring the authentication key Kn was revealed) manufactured, for example are not regular by the method of registering two or more authentication keys Kn collectively.

[0050]If the output of the contents from the contents protecting part 25 to application is detected and the owner of the copyright of contents and the administrator of a ciphering system are notified of the number of times via the Internet etc., It becomes possible to having used contents and a ciphering system to charge a user or to grasp the operating condition of a ciphering system.

[0051]This invention can be applied to the isochronous packet of the contents transmitted to an IEEE1394 bus, an asynchronous packet, and the packet of the contents transmitted to other transmission media.

[0052]A user can be provided with the computer program which performs each above-mentioned processing via network distribution media, such as the Internet and a digital satellite, besides the distribution medium which consists of information recording media, such as a magnetic disk and CD-ROM.

[0053] [Effect of the Invention]As mentioned above, according to the information processing equipment according to claim 1, the information processing method according to claim 3, and the distribution medium according to claim 4. Judge the justification of an application program using an authentication key, and it corresponds to the decided result, Since the contents enciphered with the encryption key enciphered

using the secret key and the encryption key were supplied to the application program, it becomes possible to deter the illegal use of contents.

[Claim(s)]

[Claim 1]In information processing equipment which executes an application program which can edit contents to which copyright information is added, and has an authentication key and a secret key, An encryption key creating means which generates an encryption key using a source key corresponding to said copyright information added to said contents inputted, An encoding means which enciphers said contents using said encryption key, and a judging means which judges the justification of said application program using said authentication key inputted from said application program, A secret key generating means which generates a secret key using an authentication key inputted from said application program, Information processing equipment including a feeding means which supplies said encryption key enciphered using said secret key which said secret key generating means generated, and said contents enciphered by said encoding means to said application program corresponding to a decided result of said judging means.

[Claim 2]The information processing equipment according to claim 1, wherein said judging means judges the justification of said authentication key by referring to a RIBOKESHON list.

[Claim 3]An information processing method of information processing equipment which executes an application program which can edit contents to which copyright information is added, and has an authentication key and a secret key characterized by comprising the following.

An encryption key generation step which generates an encryption key using a source key corresponding to said copyright information added to said contents inputted.

An encryption step which enciphers said contents using said encryption key.

A determination step which judges the justification of said application program using said authentication key inputted from said application program.

A secret key generation step which generates a secret key using an authentication key inputted from said application program.

A supply step which supplies said encryption key enciphered using said secret key generated by said secret key generation step, and said contents enciphered at said encryption step to said application program corresponding to a decided result of said

determination step.

[Claim 4]A distribution medium providing a program which a computer characterized by comprising the following which performs processing can read.

To information processing equipment which executes an application program which can edit contents to which copyright information is added, and has an authentication key and a secret key. An encryption key generation step which generates an encryption key using a source key corresponding to said copyright information added to said contents inputted.

An encryption step which enciphers said contents using said encryption key.

A determination step which judges the justification of said application program using said authentication key inputted from said application program.

A secret key generation step which generates a secret key using an authentication key inputted from said application program, A supply step which supplies said encryption key enciphered using said secret key generated by said secret key generation step, and said contents enciphered at said encryption step to said application program corresponding to a decided result of said determination step.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-332742

(P2000-332742A)

(43)公開日 平成12年11月30日(2000.11.30)

(S) Int.Cl. ⁷	識別記号	F I	テラコード ^(参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 D 0 4 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	3 2 0 B 5 J 1 0 4
G 1 1 B 20/10		G 1 1 B 20/10	6 4 0 Z 9 A 0 0 1
			H
		審査請求 未請求 請求項の数 4	〇 L (全 9 頁) 最終頁に続く

(21) 出願番号	特願平11-136695	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川 6 丁目 7 番35号
(22) 出願日	平成11年 5 月18日 (1999. 5. 18)	(72) 発明者	濱田 一郎 東京都品川区北品川 6 丁目 7 番35号 ソニー株式会社内
		(72) 発明者	藤井 麻子 東京都品川区北品川 6 丁目 7 番35号 ソニー株式会社内
		(74) 代理人	100082131 弁理士 稲本 義雄

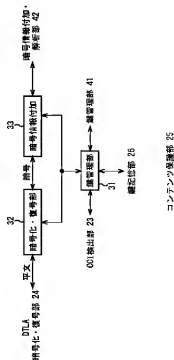
最終頁に続く

(54)【発明の名称】 情報処理装置および方法、並びに提供媒体

(57) 【要約】

【課題】 コンテンツの不正利用を抑止する。

【解決手段】 鍵管理部 3 1 は、アプリケーションが有する認証鍵 K a が正規のものであるかを判定し、正規のものであると判定したときだけ、アプリケーションとのコンテンツの授受を実行するように、コンテンツ保護部 2 5 を制御する。暗号化・復号部 3 2 は、復号されているコンテンツを、鍵管理部 3 1 から入力される暗号鍵 K c を用いて暗号化し、暗号情報付加部 3 3 へ出力する。暗号情報付加部 3 3 は、暗号化・復号部 3 2 からの暗号化されたコンテンツに、暗号情報を付加して、アプリケーションへ出力する。



【特許請求の範囲】

【請求項1】 著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置において、

入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成手段と、

前記暗号鍵を用いて前記コンテンツを暗号化する暗号化手段と、

前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定手段と、

前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成手段と、

前記秘密鍵生成手段が生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化手段により暗号化された前記コンテンツを、前記判定手段の判定結果に対応して、前記アプリケーションプログラムに供給する供給手段とを含むことを特徴とする情報処理装置。

【請求項2】 前記判定手段は、リポジトリリストを参照することにより前記認証鍵の正当性を判定することを特徴とする請求項1に記載の情報処理装置。

【請求項3】 著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置の情報処理方法において、

入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵を用いて前記コンテンツを暗号化する暗号化ステップと、

前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定ステップと、

前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、

前記秘密鍵生成ステップで生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化ステップで暗号化した前記コンテンツを、前記判定ステップの判定結果に対応して、前記アプリケーションプログラムに供給する供給ステップとを含むことを特徴とする情報処理方法。

【請求項4】 著作権情報が付加されているコンテンツを編集可能であり、かつ、認証鍵および秘密鍵を有するアプリケーションプログラムを実行する情報処理装置に、

入力される前記コンテンツに付加されている前記著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、

前記暗号鍵を用いて前記コンテンツを暗号化する暗号化ステップと、

前記アプリケーションプログラムから入力される前記認証鍵を用いて前記アプリケーションプログラムの正当性を判定する判定ステップと、

前記アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、

前記秘密鍵生成ステップで生成した前記秘密鍵を用いて暗号化した前記暗号鍵、および前記暗号化ステップで暗号化した前記コンテンツを、前記判定ステップの判定結果に対応して、前記アプリケーションプログラムに供給する供給ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、コンテンツの不正利用を抑制する場合に用いて好適な情報処理装置および方法、並びに提供媒体に関する。

【0002】

【従来の技術】 従来、著作権が保護されているコンテンツ（例えば、CD(Compact Disc)に記録されているオーディオデータ、DVD(Digital Versatile Disc)に記録されているAVデータ等）が不正に複製されることを抑制するために、コンテンツを記録可能な装置（例えば、MD(Mini Disc)レコーダ、CD-Rレコーダ、DV(Digital Video)レコーダ等）には、SCMS(Serial Copy Management System)、またはCGMS(Copy Generation Management System)が採用されている。SCMSやCGMSにおいては、コンテンツに所定の情報を付加し、その情報に基づいてコピー可能な回数を制限している。

【0003】 また、最近、コンテンツを再生、または記録するAV装置とパーソナルコンピュータとの間で、IEEE 1394バスを介してコンテンツを通信することが可能となった。さらに、パーソナルコンピュータにおいては、CPU(Central Processing Unit)の高速化やハードディスクの大容量化にもない、上述したコンテンツを再生し、記録し、さらに編集することが可能となった。

【0004】

【発明が解決しようとする課題】 したがって、パーソナルコンピュータに、上述したコンテンツに付加されている情報を意図的に改ざんするような不正なアプリケーションプログラムがインストールされている場合、コンテンツが違法にコピーされてしまうことを抑止できない課題があった。

【0005】 本発明はこのような状況に鑑みてなされたものであり、パーソナルコンピュータにおいて、アプリケーションプログラムに供給される直前のコンテンツを暗号化することにより、不正なアプリケーションプログ

ラムを用いたコンテンツの不正利用を抑止できるようにするものである。

【0006】

【課題を解決するための手段】請求項1に記載の情報処理装置は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成手段と、暗号鍵を用いてコンテンツを暗号化する暗号化手段と、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定手段と、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成手段と、秘密鍵生成手段が生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化手段により暗号化されたコンテンツを、判定手段の判定結果に対応して、アプリケーションプログラムに供給する供給手段とを含むことを特徴とする。

【0007】請求項3に記載の情報処理方法は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、暗号鍵を用いてコンテンツを暗号化する暗号化ステップと、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定ステップと、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、秘密鍵生成ステップで生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化ステップで暗号化したコンテンツを、判定ステップの判定結果に対応して、アプリケーションプログラムに供給する供給ステップとを含むことを特徴とする。

【0008】請求項4に記載の提供媒体は、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵を生成する暗号鍵生成ステップと、暗号鍵を用いてコンテンツを暗号化する暗号化ステップと、アプリケーションプログラムから入力される認証鍵を用いてアプリケーションプログラムの正当性を判定する判定ステップと、アプリケーションプログラムから入力される認証鍵を用いて秘密鍵を生成する秘密鍵生成ステップと、秘密鍵生成ステップで生成した秘密鍵を用いて暗号化した暗号鍵、および暗号化ステップで暗号化したコンテンツを、判定ステップの判定結果に対応して、アプリケーションプログラムに供給する供給ステップとを含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0009】請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載の提供媒体においては、入力されるコンテンツに付加されている著作権情報に対応するソース鍵を用いて暗号鍵が生成され、暗号鍵を用いてコンテンツが暗号化される。また、アプリケーションプログラムから入力される認証鍵を用

いて秘密鍵が生成されて、アプリケーションプログラムの正当性が判定され、その判定結果に対応して、秘密鍵を用いて暗号化した暗号鍵、および暗号化されているコンテンツが、アプリケーションプログラムに供給される。

【0010】

【発明の実施の形態】本発明を適用したパーソナルコンピュータの構成例について、図1を参照して説明する。このパーソナルコンピュータ(PC)1は、IEEE1394バス2を介して、コンテンツを扱うことが可能な機器(例えば、図1に示すようなDVレコーダ(DVR)3、セットトップボックス(STB)4、およびハードディスク(HDD)5等)と接続されている。なお、IEEE1394バス2を介して通信されるコンテンツは、CPiWG(CopyProtection Technical Working Group)で推奨されるライセンス管理会社DTLA(Digital Transmission Licensing Administrator)がライセンスする方式(以下、DTLA方式と記述する)に基づいて暗号化されている。

【0011】パーソナルコンピュータ1は、バス16を介して接続されている、IEEE1394インタフェース11、CPU12、RAM13、ROM14、およびハードディスク15から構成される。IEEE1394インタフェース11は、IEEE1394バス2を介して、他の機器(DVR3等)から入力されるコンテンツを、パーソナルコンピュータ1で起動されている、コンテンツに対して再生、記録、編集等が可能なアプリケーションプログラム(以下、起動されている、コンテンツに対して再生、記録、編集等が可能なアプリケーションプログラムを、単にアプリケーションと記述する)に供給する。また、IEEE1394インタフェース11は、アプリケーションが処理したコンテンツを、IEEE1394バス2を介して他の機器に出力する。

【0012】なお、アプリケーションプログラムは、ハードディスク15に記憶されており、ROM14に記憶されているBIOSに基づくCPU12の制御によって、RAM13に転送されて起動される。また、このアプリケーションプログラムに対しては、DTLAのような暗号システムの管理者から固有の認証鍵K_nが与えられているが、この認証鍵K_nを得るためには、アプリケーションプログラムの制作元、およびユーザが、著作権が保護されているコンテンツを不正に利用しない旨を契約書等で誓約する必要がある。また、本明細書においてシステム用語は、複数の装置、手段などにより構成される全体的な装置を意味するものである。

【0013】ここで、認証鍵K_nには、IDとSignatureの対となる2値が含まれており、一方に所定の演算式を適用した結果が他方となっている。また、双方に所定の演算式を適用することにより、正しい対であることが確認できる。この所定の演算式を知っている、すなわち、認証鍵K_nの正当性を判定できるのは、鍵管理部31(図3)だけである。また、所定の演算式を、IDとSign

atureを用いた逆算により求めることは非常に困難であるので、事実上、認証鍵K_nを偽造することは不可能である。

【0014】図2は、IEEE1394インタフェース11の詳細な構成例を示している。制御部21は、IEEE1394インタフェース11の各部を制御する。入出力部22は、IEEE1394バス2から入力される、DTLA方式で暗号化されているコンテンツを受け付けてCCI(Copy Control Information)検出部23に出力する。CCI検出部23は、入出力部22から入力されるコンテンツをDTLA暗号化・復号部24に供給するが、その際、コンテンツのヘッダに記録されているCCI(2ビット)を検出して、制御部21、DTLA暗号化・復号部24、およびコンテンツ保護部25に供給する。

【0015】なお、CCIは、自身が付加されているコンテンツに対して許可されているコピーの制御を示す情報であり、00、10、01、11の4種類のステートがある。CCIが00(Copy free)である場合、対応するコンテンツに対しては無制限回数のコピーが許可されていることを意味している。CCIのステートが10(One Generation Copy Possible)である場合、対応するコンテンツに対しては1回だけコピーが許可されていることを意味している。CCIのステートが01(No More Copy)である場合、対応するコンテンツは、CCIのステートが10であるコンテンツを複製したもの(2世代目)であって、これに対してはコピーが許可されていないことを意味している。CCIのステートが11(Never copy)である場合、対応するコンテンツに対してはコピーが許可されていないことを意味している。

【0016】DTLA暗号化・復号部24は、CCI検出部23から入力されるDTLA方式で暗号化されているコンテンツを復号し、コンテンツ保護部25に出力する。また、DTLA暗号化・復号部24は、コンテンツ保護部25から入力されるコンテンツを、DTLA方式の用いて暗号化して入出力部22に出力する。なお、DTLA暗号化・復号部24における暗号化および復号は、DTLA暗号化・復号部24とコンテンツを出力した装置(DVR3等)の間におけるDTLA方式で定義されている相互認証作業が終了した後に実行される。

【0017】コンテンツ保護部25は、DTLA暗号化・復号部24から入力されるコンテンツを暗号化してアプリケーションに供給する。また、コンテンツ保護部25は、アプリケーションから入力される、暗号化されているコンテンツを復号してDTLA暗号化・復号部24に供給する。鍵記憶部26は、コンテンツ保護部25における暗号化処理に用いられるソース鍵K_sを、CCIのステート毎に複数個記憶している。

【0018】図3は、コンテンツ保護部25の詳細な構成例を示している。鍵管理部31は、アプリケーションの鍵管理部41(図4)から入力される認証鍵K_nが正

規のものであるかを判定し、認証鍵K_nが正規のものであると判定したときだけ、アプリケーションとのコンテンツの授受を実行するように、コンテンツ保護部25の各部を制御する。

【0019】すなわち、鍵管理部31は、アプリケーションからの認証鍵K_nに含まれるIDに所定の演算式を適用し、その結果が対応するSignatureと等しいか否かを判定し、演算結果がSignatureと等しい(認証鍵K_nが正規のものである)と判定した場合、さらに、IDとSignatureに所定の演算式を適用することにより、正しい対であるか否かを判定し、正しい対であると判定した場合、CCI検出部23から入力されるCCIのステートに対応するソース鍵K_sを読み出し、ソース鍵K_sおよび乱数を用いて暗号鍵K_cを生成して、暗号化・復号部32に供給する。なお、暗号鍵K_cは、所定の周期(例えば、30秒間乃至120秒間)毎に更新される。また、鍵管理部31は、CCIのステートを、暗号鍵K_cを更新する毎に暗号情報付加部33に出力する。さらに、鍵管理部31は、アプリケーションの鍵管理部41から入力される認証鍵等の秘密鍵K_a算出用情報に基づいて秘密鍵K_aを生成し、暗号鍵K_cを秘密鍵K_aを用いて暗号化して鍵管理部41に出力する。

【0020】暗号化・復号部32は、DTLA暗号化・復号部24からの復号されているコンテンツを、鍵管理部31からの暗号鍵K_cを用いて暗号化し、暗号情報付加部33に出力する。また、暗号化・復号部32は、暗号情報付加部33からの、暗号化されているコンテンツを復号してDTLA暗号化・復号部24に出力する。

【0021】暗号情報付加部33は、暗号化・復号部32からの暗号化されたコンテンツに、CCIのステート(2ビット)、暗号鍵K_cが更新される毎に切り替えられるevenまたはodd(1ビット)の暗号情報を付加して、アプリケーションの暗号情報解析部42(図4)に出力する。また、暗号情報付加部33は、暗号情報解析部42からの暗号化されたコンテンツを、暗号化・復号部32に出力する。

【0022】図4は、コンテンツに対して再生、記録、編集等が可能なアプリケーションの機能ブロック図を示している。鍵管理部41は、アプリケーションプログラムに対して与えられている認証鍵K_nを記憶しており、アプリケーションがコンテンツの授受を開始する前に、記憶している認証鍵K_nを、秘密鍵K_a算出用情報とともに、コンテンツ保護部25の鍵管理部31に出力する。また、鍵管理部41は、暗号情報解析部42から入力される、暗号情報に含まれる暗号鍵K_cの更新を示す情報(evenまたはodd)が切り替えられたか否かを示す情報に対応して、鍵管理部31からの秘密鍵K_aで暗号化されている暗号鍵K_cを復号し、暗号化・復号部43に出力する。

【0023】暗号情報解析部42は、暗号情報付加部3

3から入力される、暗号鍵Kcで暗号化されているコンテンツを暗号化・復号部43に出力し、付加されている暗号情報を鍵管理部41に出力する。また、暗号情報解析部42は、暗号化・復号部43からの暗号化されたコンテンツを暗号情報付加部33に出力する。

【0024】暗号化・復号部43は、暗号情報解析部42からの入力される暗号鍵Kcで暗号化されているコンテンツを、鍵管理部41からの暗号鍵Kcを用いて復号し、コンテンツ処理部44に出力する。また、暗号化・復号部43は、コンテンツ処理部44から入力されるコンテンツを暗号化し、暗号情報解析部42に出力する。

【0025】コンテンツ処理部44は、入力されたコンテンツに対して、ユーザの操作に対応する処理（再生、記録、または編集等）を実行する。なお、コンテンツ処理部44には、暗号情報解析部42が解析した暗号情報に含まれるC(1)が供給されるので、コンテンツ処理部44においては、C(1)に反するような処理（制限回数を越えるコピー等）は実行されない。

【0026】なお、IEEE1394インタフェース11を1個のLSI (Large Scale Integrated circuit) で実現すれば、回路の途中から復号されたコンテンツを読み出すような不正行為を抑止することが可能となる。

【0027】次に、アプリケーションにコンテンツを入力する処理について、図5のフローチャートを参照して説明する。この入力処理は、IEEE1394インタフェース11にDTLA方式で暗号化されているコンテンツが入力され、そのC(1)が、C(1)検出部23で検出されてコンテンツ保護部25の鍵管理部31に入力され、DTLA方式で暗号化されているコンテンツが、DTLA暗号化・復号部24で復号されてコンテンツ保護部25の暗号化・復号部32に入力された後に実行される。

【0028】ステップS1において、アプリケーションの鍵管理部41は、コンテンツ入力の要求、記憶している認証鍵Kn、および秘密鍵Ka算出用情報を入力し、それらを、コンテンツ保護部25の鍵管理部31が受け付ける。

【0029】ステップS2において、鍵管理部31は、鍵管理部41からの認証鍵Knが正規のものであるかを判定し、認証鍵Knが正規のものであると判定した場合、ステップS3に進む。

【0030】ステップS3において、鍵管理部31は、C(1)のスタートに対応するソース鍵Ksを鍵記憶部26から読み出して、ソース鍵Ksと乱数を用いて暗号鍵Kcを生成し、暗号化・復号部32に出力する。また、鍵管理部31は、暗号鍵Kcを更新するタイミングを計測するタイマを0にリセットする。

【0031】ステップS4において、鍵管理部31は、秘密鍵Ka算出用情報を用いて秘密鍵Kaを生成し、さらに、秘密鍵Kaを用いて暗号鍵Kcを暗号化し、アプリケーションの鍵管理部41に出力する。鍵管理部41

は、暗号鍵Kcを復号する。

【0032】ステップS5において、暗号化・復号部32は、DTLA暗号化・復号部24からの復号されているコンテンツを、鍵管理部31からの暗号鍵Kcを用いて暗号化し、暗号情報付加部33に出力する。

【0033】ステップS6において、暗号情報付加部33は、C(1)のスタート、暗号鍵Kcの更新を示す情報（いまの場合、暗号鍵Kcは更新されていないのでeven）から成る暗号情報を生成し、暗号化・復号部32からの暗号化されたコンテンツに付加して、アプリケーションの暗号情報解析部42に出力する。暗号情報解析部42は、暗号情報に含まれる、暗号鍵Kcの更新を示す情報が切り替えられているかを判定し、判定結果を鍵管理部41に出力する。鍵管理部41は、この判定結果に基づき、いまの暗号鍵Kcを暗号化・復号部43に供給する。暗号化・復号部43は、暗号鍵Kcを用いてコンテンツを復号し、コンテンツ処理部44に出力する。

【0034】ステップS7において、鍵管理部31は、全てのコンテンツをコンテンツ保護部25からアプリケーションに出力したか否かを判定し、全てのコンテンツを出力していないと判定した場合、ステップS8に進む。ステップS8において、鍵管理部31は、自己のタイマを参照することにより、いまの暗号鍵Kcが用いられている時間を検知し、その時間が所定時間（30秒間乃至120秒間）を経過したか否かを判定する。いまの暗号鍵Kcが用いられている時間が所定時間を経過していないと判定された場合、ステップS5に戻り、それ以降の処理が繰り返される。

【0035】その後、ステップS8において、いまの暗号鍵Kcの使用時間が所定時間を経過したと判定された場合、ステップS9に進む。ステップS9において、鍵管理部31は、ソース鍵Ksと、再度発生させた乱数を用いて暗号鍵Kcを生成（更新）し、暗号化・復号部32に出力する。また、鍵管理部31は、自己のタイマを0にリセットする。

【0036】その後、ステップS4に戻り、ステップS7で全てのコンテンツを出力したと判定されるまで、以降の処理が繰り返される。ただし、ステップS6で付加される暗号情報に含まれる、暗号鍵Kcの更新を示す情報は、ステップS9で暗号鍵Kcが更新されているのでevenからoddに切り替えられる。この暗号鍵Kcの更新を示す情報に対応して、鍵管理部41から暗号化・復号部32に供給される暗号鍵Kcも更新される。

【0037】なお、ステップS2において、認証鍵Knが正規のものではないと判定された場合、ステップS10に進む。ステップS10において、鍵管理部31は、アプリケーションの鍵管理部41に対して、認証は不可能である旨を通知する。

【0038】次に、アプリケーションで処理されたコン

テンツをIEEE1394バス2に出力する処理について、図6のフローチャートを参照して説明する。この出力処理は、アプリケーションのコンテンツ処理部44において編集されたコンテンツが暗号化・復号部43に入力された後に実行される。

【0039】ステップS21において、アプリケーションの鍵管理部41は、コンテンツ出力の要求、記憶している認証鍵K_n、秘密鍵K_a算出用情報、および出力するコンテンツに対して設定するCCIのステートを、コンテンツ保護部25の鍵管理部31に出力する。

【0040】ステップS22において、鍵管理部31は、鍵管理部41からの認証鍵K_nが正規のものであるか否かを判定し、認証鍵K_nが正規のものであると判定した場合、ステップS23に進む。

【0041】ステップS23において、鍵管理部31は、鍵管理部41から入力されたCCIのステートに対応するソース鍵K_sを鍵記憶部26から読み出して、ソース鍵K_sと乱数を用いて暗号鍵K_cを生成し、暗号化・復号部32に供給する。ステップS24において、鍵管理部31は、鍵管理部41からの秘密鍵K_a算出用情報を用いて秘密鍵K_aを生成し、さらに、秘密鍵K_aを用いて、ステップS22で生成した暗号鍵K_cを暗号化し、アプリケーションの鍵管理部41に出力する。鍵管理部41は、暗号鍵K_cを復号して、暗号化・復号部43に出力する。

【0042】ステップS25において、アプリケーションの暗号化・復号部43は、鍵管理部41からの暗号鍵K_cを用いて、コンテンツ処理部44から入力されたコンテンツを暗号化し、暗号情報解析部42および暗号情報付加部33を介して、暗号化・復号部32に出力する。

【0043】ステップS26において、暗号化・復号部32は、ステップS23で鍵管理部31から入力された暗号鍵K_cを用いて、アプリケーション（暗号化・復号部43）からの暗号化されたコンテンツを復号し、DTLA暗号化・復号部24に出力する。

【0044】ステップS27において、DTLA暗号化・復号部24は、コンテンツ保護部25の暗号化・復号部32から入力された復号されているコンテンツを、DTLA方式で暗号化し、入出力部22に出力する。

【0045】ステップS28において、入出力部22は、DTLA暗号化・復号部24からのDTLA方式で暗号化されているコンテンツをIEEE1394バス2に出力する。

【0046】なお、ステップS22において、認証鍵K_nが正規のものではないと判定された場合、ステップS29に進む。ステップS29において、鍵管理部31は、アプリケーションの鍵管理部41に対して、認証は不可能である旨を通知する。

【0047】また、この出力処理においても、上述した入力処理と同様、周期的に暗号鍵K_cを変更するように

してもよい。

【0048】以上のように、本実施の形態によれば、正規の認証鍵K_nを持っているアプリケーションに対してだけ、IEEE1394インタフェース11のコンテンツ保護部25は、コンテンツの授受を行うようになっている。しかしながら、コンテンツの違法コピー等を実行可能なアプリケーションが、何らかの方法により、正規の認証鍵K_nを取得し、コンテンツが不正に利用されてしまうことも考えられる。そこで、本発明においては、認証鍵K_nの正当性を判定するコンテンツ保護部25の鍵管理部31に、不正に使用された認証鍵K_nが登録されているリポーションリストを記憶させ、認証処理の際、鍵管理部31は、認証鍵K_nに含まれるIDとSignatureの整合性の判定に加えて、リポーションリストとの照合を実行するようにして、リポーションリストに登録されている認証鍵K_nは、IDとSignatureが対となっていないても正規なものであると判定されないようになされている。

【0049】なお、このリポーションリストに関しては、その最新のものをインターネットやIEEE1394バス2等のネットワークを介して、鍵管理部31に配信する方法が考えられる。また、このリポーションリストの利用方法としては、認証鍵K_nを個々に登録する方法と、複数の認証鍵K_nをまとめて登録する方法（例えば、認証鍵K_nのIDのMSB(Most Significant Bit)側の所定ビットを指定する等）が考えられる。複数の認証鍵K_nをまとめて登録する方法により、例えば、特定のソフトウェア（認証鍵K_nを取得する際に契約した規約に対する違反が発覚したソフトウェア）が製作した全てのアプリケーションを、正規なものではないと判定させることが可能となる。

【0050】また、コンテンツ保護部25からアプリケーションへのコンテンツの出力を検知し、その回数をインターネット等を介して、コンテンツの著作権の所有者や暗号システムの管理者に通知するようにすれば、コンテンツや暗号システムを使用したことに対して、ユーザに課金することや、暗号システムの使用状況を把握することが可能となる。

【0051】なお、本発明は、IEEE1394バスに伝送されるコンテンツのアイソクロナスパケットおよびアシンクロナスパケット、並びに、他の伝送媒体に伝送されるコンテンツのパケットに対して適用することが可能である。

【0052】また、上記各処理を行うコンピュータプログラムは、磁気ディスク、CD-ROM等の情報記録媒体よりなる提供媒体のほか、インターネット、デジタル衛星などのネットワーク提供媒体を介してユーザに提供することができる。

【0053】

【発明の効果】以上のように、請求項1に記載の情報処

理装置、請求項 3 に記載の情報処理方法、および請求項 4 に記載の提供媒体によれば、認証鍵を用いてアプリケーションプログラムの正当性を判定し、その判定結果に対応して、秘密鍵を用いて暗号化した暗号鍵、および暗号鍵で暗号化されているコンテンツを、アプリケーションプログラムに供給するようにしたので、コンテンツの不正利用を抑止することが可能となる。

【図面の簡単な説明】

【図 1】 本発明を適用したパーソナルコンピュータ 1 の構成例を示すブロック図である。

【図 2】 図 1 の IEEE1394 インタフェース 11 の構成例を示すブロック図である。

【図 3】 図 2 のコンテンツ保護部 25 の構成例を示すブロック図である。

【図 4】 パーソナルコンピュータ 1 で起動されているアプリケーションの機能を示すブロック図である。

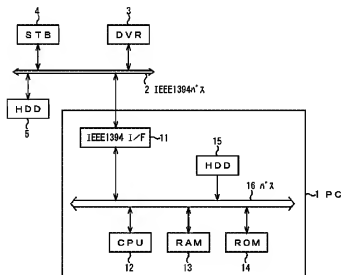
【図 5】 図 1 の IEEE1394 インタフェース 11 の動作を説明するフローチャートである。

【図 6】 図 1 の IEEE1394 インタフェース 11 の動作を説明するフローチャートである。

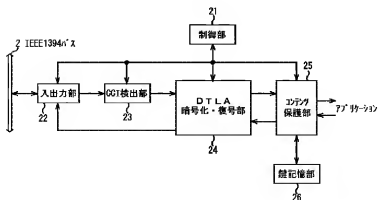
【符号の説明】

- 1 パーソナルコンピュータ、 2 IEEE1394バス、
11 IEEE1394インタフェース、 25 コンテンツ保護部、
31 鍵管理部、 32 暗号化・復号部、
33 暗号情報付加部、 41 鍵管理部、 42 暗号情報解析部、
43 暗号化・復号部、 44 コンテンツ処理部

【図 1】



【図 2】



```

graph TD
    DTLA[DTLA] --> 24[暗号化・復号部 24]
    24 --> 32[暗号部 32]
    32 --> 33[暗号情報付加部 33]
    33 --> 42[暗号情報付加・解除部 42]
    32 <--> 33
    32 <--> MC[管理制御部]
    33 <--> MC
    42 <--> MC
    MC <--> 23[CCU検出部 23]
    MC <--> 26[鍵記憶部 26]

```

```

graph TD
    SMU[システム管理部]
    SFA[信号特徴解析部]
    ED[符号化・復号部]
    CMU[コンテンツ管理部]

    SMU <--> SFA
    SMU <--> ED
    SMU <--> CMU
    SFA <--> ED
    ED <--> CMU

```

```

graph TD
    Start([出力処理開始]) --> S21[S21  
ソング出力要求  
認証鍵Ka  
秘密鍵Ka 出用情報C1情報を出力]
    S21 --> S22{S22  
認証 OK ?}
    S22 -- Yes --> S23[S23  
ソース鍵Ka を用いて暗号鍵Kc を演算]
    S22 -- No --> S29[S29  
認証不可を通知]
    S23 --> S24[S24  
秘密鍵Ka を用い、  
暗号鍵Kc を暗号化して出力]
    S24 --> S25[S25  
アプリケーションが暗号鍵Kc を用いて  
コンテンツを暗号化]
    S25 --> S26[S26  
暗号鍵Kc を用いてコンテンツを復号]
    S26 --> S27[S27  
コンテンツをDITAに基づいて暗号化]
    S27 --> S28[S28  
出力]
    S28 --> End([終了])
  
```

出力処理開始

S21
ソング出力要求
認証鍵Ka
秘密鍵Ka 出用情報C1情報を出力

S22
認証 OK ?

Yes

S23
ソース鍵Ka を用いて暗号鍵Kc を演算

S24
秘密鍵Ka を用い、
暗号鍵Kc を暗号化して出力

S25
アプリケーションが暗号鍵Kc を用いて
コンテンツを暗号化

S26
暗号鍵Kc を用いてコンテンツを復号

S27
コンテンツをDITAに基づいて暗号化

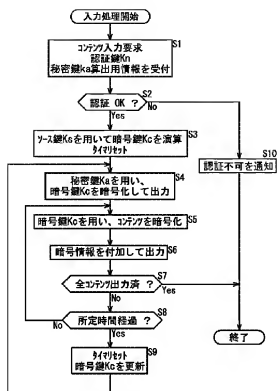
S28
出力

終了

No

S29
認証不可を通知

【図5】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

ターコード (参考)

H 0 4 L 9/32

H 0 4 L 9/00

6 0 1 E

6 7 3 B

F ターム (参考) 5B017 AA06 BA05 BA07 BB02 BB03
 BB10 CA07 CA09 CA16
 5D044 BC01 CC04 DE17 GK17 HL01
 5J104 AA07 AA16 EA04 EA17 KA02
 MA02 NA02 NA32 PA14
 9A001 BB01 BB03 BB04 BB05 CC05
 DD06 EE03 GG22 JJ25 KK37
 LL03